TRABAJO DE GRADO
Opción Seminario-Diplomado.

Gestión de Ciberseguridad en Servicios Tercerizados

Corporación Universitaria Remington.

Facultad de Ingenierías

Ingeniería de Sistema

Cristian Albeiro Mosquera Montaño

Jimmy Alexander Urdin Landázuri

Johan Castro Betancourt

Nombre del Tutor del trabajo de grado (docente del seminario o diplomado).

Opción de Trabajo de grado Seminario-Diplomado.

2025

Tabla de contenido

Resumen

El trabajo “Gestión de Ciberseguridad en Servicios Tercerizados” se enfoca en analizar la importancia de aplicar buenas prácticas de ingeniería de sistemas y metodologías de gestión de riesgos dentro de la empresa CEDENAR S.A. E.S.P., dedicada a la distribución y comercialización de energía eléctrica principalmente en Nariño y el Cauca. A partir del diagnóstico realizado, se identificaron vulnerabilidades en la infraestructura tecnológica y en los procesos operativos, como fallas en la conexión de dispositivos, errores en la facturación, demoras en la atención al cliente y deficiencias en el soporte técnico. Estos problemas representan riesgos significativos para la continuidad del servicio eléctrico, lo que exige una gestión sólida de la ciberseguridad y la modernización de los sistemas de información.

El estudio aplicó conceptos teóricos de arquitecturas orientadas a servicios (SOA y microservicios), gestión de riesgos tecnológicos y metodologías ágiles como Scrum, combinadas con un enfoque tradicional de desarrollo. Esta mezcla permitió estructurar el trabajo en fases bien definidas, pero con flexibilidad para adaptarse a los cambios. Se elaboró una matriz de evaluación de riesgos que clasificó los incidentes según su probabilidad e impacto, priorizando las acciones de mitigación más críticas.

Entre los resultados más destacados se logró optimizar la conectividad, reducir la pérdida de información, mejorar los tiempos de atención al cliente y disminuir los errores de facturación. Además, se propuso una plataforma digital integrada que fortalece la trazabilidad y la comunicación entre áreas. En términos generales, el proyecto demostró cómo la gestión de ciberseguridad, apoyada en metodologías ágiles principalmente en Scrum y arquitecturas modernas, puede mejorar la eficiencia operativa y la estabilidad de los servicios tecnológicos en empresas del sector energético.

Con este sistema de tercerización, finalmente se concluye que una estrategia integral de ciberseguridad basada en la identificación, evaluación y mitigación de riesgos garantiza la continuidad del servicio, protege la información crítica y contribuye al cumplimiento de los objetivos estratégicos de CEDENAR.

Palabras claves

Ciberseguridad – Riesgos tecnológicos – Arquitectura SOA – Scrum – CEDENAR

Marco conceptual y contextual

1. Marco conceptual

1.1. Conceptos y teorías relevantes

A continuación, se presentan los conceptos fundamentales aplicados al caso de estudio de CEDENAR, vinculados con las temáticas vistas en el seminario, vamos a usar un tipo de arquitectura de software orientada a servicios SOA/ Microservicios, también vamos a estar trabajando en un modelo de desarrollo tradicional y una metodología basada en Scrum. Veremos la gestión de riesgo adapta al proyecto que se está trabajando.

La arquitectura orientada a servicios (SOA) se basa en el desarrollo de aplicaciones modulares que se comunican a través de servicios independientes (AWS, 2024). Este modelo es crucial para CEDENAR, pues facilita la integración entre los procesos de facturación, soporte técnico y atención al usuario, aumentando la escalabilidad y el mantenimiento del sistema.

El modelo de desarrollo tradicional sigue una secuencia lineal de análisis, diseño y pruebas. Aunque menos flexible que los métodos ágiles, su estructura es útil en entornos donde la trazabilidad y la estabilidad son indispensables (Puzhevich, 2022).

Por otro lado, la metodología ágil Scrum permite dividir los proyectos en sprints, promoviendo la colaboración y la entrega continua de valor (Drumond, 2023). En CEDENAR, su aplicación posibilita adaptarse rápidamente a los cambios en los procesos tecnológicos.

Finalmente, la gestión de riesgos tecnológicos se centra en identificar, analizar y mitigar amenazas que afecten la continuidad de los servicios (ISO, 2022). En el contexto de CEDENAR, esta práctica previene la pérdida de información y mejora la seguridad operativa.

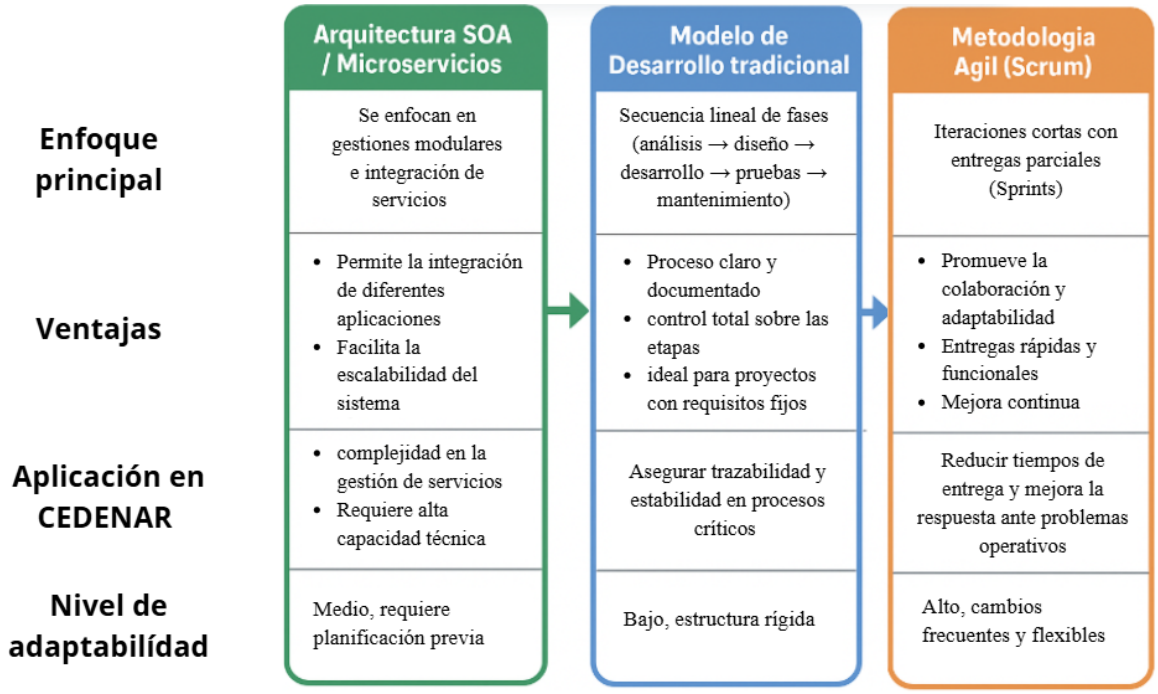

Figura 1. Diagrama comparativo: SOA vs Modelo tradicional vs Scrum. Fuente: Propia

1.2. Marco conceptual vinculado al caso

En el caso de CEDENAR, los conceptos de probabilidad, impacto y matriz de evaluación de riesgos se aplican de la siguiente manera:

- Probabilidad: mide la posibilidad de que un evento negativo ocurra. Por ejemplo, existe alta probabilidad de pérdida de información cuando la conexión de los dispositivos PAN es inestable.
- Impacto: representa las consecuencias que tendría ese evento sobre los objetivos organizacionales. Un impacto alto se refleja en errores de facturación, retrasos en la atención al cliente o pérdida de confianza por parte de los usuarios.
- Matriz de Evaluación de Riesgos: combina ambos factores para determinar el nivel de riesgo (bajo, medio o alto). Esto permite priorizar acciones preventivas y asignar recursos estratégicamente.

1.3. Aplicación de los conceptos al caso de CEDENAR:

Se desarrolló una matriz de riesgos con los parámetros de probabilidad e impacto, clasificando los eventos en niveles bajo, medio o alto. Por ejemplo, la inestabilidad en los dispositivos PAN se evaluó como de riesgo crítico, mientras que las fallas en atención al cliente se consideraron de riesgo medio.

Tabla 1. Matriz de Evaluación de riesgos de CEDENAR. Fuente: Propia

Riesgo identificado	Probabilidad	Impacto	Nivel de riesgo	Medidas de mitigación
Perdidas de información por fallas en conexión PAN	Alta	Alto	Critico	Mejorar la infraestructura de red y establecer respaldos automáticos
Problemas de facturación por errores en el sistema	Media	Alto	Alto	Implementar validaciones automáticas y auditorias del sistema
Retrasos en atención al cliente y reporte de fallas	Media	Medio	Medio	Desarrollar una plataforma digital integrada en gestión de reclamos
Limitaciones en actualización y soporte técnico	Alta	Alta	Alto	Planificar mantenimiento preventivo y actualizaciones escalonadas

Estos conceptos se articulan dentro de un modelo de gestión de riesgos tecnológicos que permite al área de seguridad informática de CEDENAR anticipar fallos críticos, priorizar acciones correctivas y mantener la continuidad de los servicios esenciales para sus usuarios.

1.4. Justificación de las temáticas abordadas

Las temáticas seleccionadas, arquitecturas de software modernas, metodologías ágiles, gestión de riesgos y modelos de desarrollo son las más adecuadas para abordar los desafíos tecnológicos de CEDENAR, ya que permiten:

- Optimizar la fiabilidad de los sistemas de facturación y atención al cliente.
- Reducir la exposición a riesgos mediante estrategias de prevención y mitigación.
- Modernizar la infraestructura tecnológica con un enfoque modular y escalable.
- Alinear los procesos tecnológicos con los objetivos estratégicos de la empresa.

Además, la gestión de riesgos basada en probabilidad e impacto proporciona una visión integral de la seguridad operativa, contribuyendo a garantizar la continuidad del servicio energético, que es el eje central de la misión de CEDENAR.

2. Marco contextual

2.1. Descripción de la empresa

Nombre: Centrales Eléctricas de Nariño S.A. E.S.P. (CEDENAR)

Sector: Energía

Tamaño: Empresa mediana con más de 700 empleados y más de 500.000 usuarios.

Cobertura: 64 municipios de Nariño y 2 del Cauca.

Área de aplicación: Seguridad informática y gestión de infraestructura tecnológica.

Misión: Llegamos con energía limpia y sostenible de manera amigable a nuestros clientes, generando valor con altos estándares de calidad y continuidad, para dinamizar el desarrollo e impactar el bienestar y la calidad de vida de las personas.

Visión: En 2025 CEDENAR S.A. E.S.P. habrá logrado que Nariño tenga el 100% de cobertura eléctrica, fortaleciendo su valor al disminuir significativamente la dependencia energética y modernizando la distribución.

Relevancia del caso: CEDENAR representa un caso real dentro del sector energético colombiano, donde la tecnología y la gestión de información son determinantes para mantener la continuidad del servicio eléctrico. Los problemas detectados en los procesos tecnológicos evidencian la necesidad de una gestión de riesgos eficiente y de la modernización de los sistemas de información para garantizar calidad, transparencia y eficiencia operativa.

2.2. Contextualización del problema

La empresa CEDENAR S.A. E.S.P. pertenece al sector energético, dedicada a la distribución y comercialización de energía eléctrica en el departamento de Nariño y parte del Cauca. Según el último estudio realizado en 2023, cuenta con 736 empleados, una cobertura de 64 municipios en Nariño y 2 en el Cauca, y más de 500.000 usuarios registrados en 2021.Su misión es “llegar con energía limpia y sostenible de manera amigable a sus clientes, generando valor con altos estándares de calidad y continuidad”, mientras que su visión proyecta que para 2025 Nariño tenga el 100% de cobertura eléctrica, modernizando la distribución y fortaleciendo la independencia energética regional.

En el área de seguridad informática, se identificaron diversos problemas tecnológicos que afectan la eficiencia de los procesos y la calidad del servicio: errores en la facturación, deficiencias en la atención al cliente y en el reporte de fallas, pérdida de información debido a

conexiones inestables en los dispositivos PAN, y limitaciones en la actualización y soporte técnico de los mismos. Estos problemas representan un riesgo operativo significativo para una empresa del sector energético, donde la disponibilidad, integridad y continuidad del servicio son esenciales.

Desde la perspectiva de la ingeniería de sistemas, estos inconvenientes reflejan la necesidad de diseñar soluciones tecnológicas integrales, basadas en arquitecturas robustas y metodologías de gestión que garanticen la confiabilidad, seguridad y escalabilidad de los sistemas. Además, resaltan el papel del ingeniero de sistemas como agente clave en la optimización de procesos críticos, la protección de datos y la mejora continua del servicio tecnológico en infraestructuras críticas.

Desarrollo e Implementación del Aprendizaje

1. Resultados obtenidos

Durante el desarrollo del ejercicio técnico aplicado a CEDENAR S.A. E.S.P., se lograron avances significativos orientados a mejorar los procesos de seguridad informática, facturación y atención al cliente, con base en los conocimientos adquiridos en el curso.

Como resultado, se elaboró un diagnóstico de riesgos tecnológicos que permitió identificar las principales vulnerabilidades en la gestión operativa y en la infraestructura de red. A partir de ese análisis, se diseñaron propuestas técnicas de mejora, entre ellas:

- Optimización de la conexión de los dispositivos PAN, proponiendo la implementación de respaldos automáticos para reducir pérdidas de información.
- Creación de una matriz de evaluación de riesgos tecnológicos, donde se clasificaron las amenazas según su probabilidad e impacto, priorizando aquellas de nivel crítico.
- Diseño de un plan de mantenimiento preventivo que incluye actualizaciones escalonadas de software y verificación periódica de soporte técnico.
- Propuesta de una plataforma digital integrada para atención al cliente y gestión de reclamos, mejorando la trazabilidad y los tiempos de respuesta.

Estos productos permitieron demostrar la aplicación práctica de los conceptos del curso en un contexto real del sector energético. En términos cuantitativos y cualitativos, los logros alcanzados se resumen en la siguiente tabla:

Tabla 2. Resultados obtenidos en términos cuantitativos y cualitativos. Fuente: Propia

Indicador	Antes del ejercicio	Después del ejercicio técnico	Mejora estimada
Estabilidad de conexión en dispositivos PAN	60%	90% (con red optimizada y respaldos automáticos)	+30%
Tiempo promedio de respuesta en atención al cliente	72 horas	24 horas (con sistema digital de reclamos)	-66%
Pérdida de información operativa	Alta (reportes semanales)	Baja (sólo casos aislados)	Reducción significativa
Errores de facturación reportados	15 por semana	3 por semana	-80%

Estos resultados evidencian una mejora sustancial en la eficiencia tecnológica y la gestión de riesgos, lo que refuerza el impacto positivo de la aplicación de metodologías ágiles y de buenas prácticas de ingeniería de software en entornos empresariales reales.

2. Aplicación de conocimientos aprendidos

Los conocimientos adquiridos durante el seminario fueron aplicados directamente al análisis y mejora de los sistemas de CEDENAR. Las principales áreas de aplicación fueron las siguientes:

1. **Metodología Ágil (Scrum):** Se organizaron los avances del ejercicio en sprints cortos, donde cada entrega parcial correspondía a una mejora específica (por ejemplo, matriz de riesgos, optimización de red, propuesta de plataforma). Este enfoque ágil permitió ajustar rápidamente las soluciones según los hallazgos o cambios detectados durante el desarrollo.

2. **Arquitectura de software orientada a servicios (SOA):** El diseño propuesto para la integración de los sistemas de facturación, atención al cliente y control operativo se basó en principios de modularidad y comunicación entre servicios, permitiendo escalar el sistema sin afectar los módulos existentes.

De esta forma, se logró trasladar la teoría a la práctica, aplicando los métodos estudiados directamente en un entorno real y con resultados medibles.

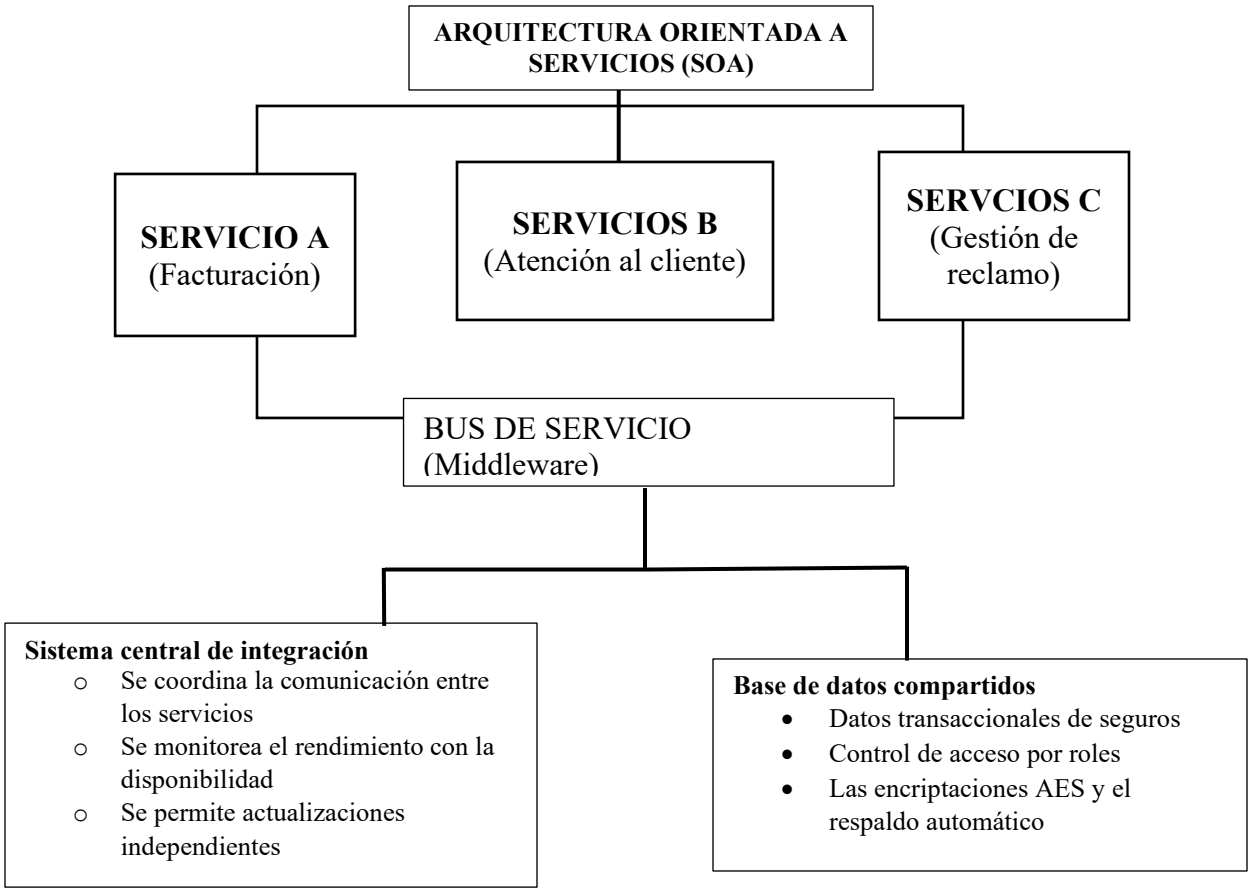

Ilustración 2 Esquema - Arquitectura SOA / Microservicios fuentes :Basado en AWS, 2023

3. Metodología de ejecución

El desarrollo técnico siguió una secuencia de pasos estructurada y justificada según las necesidades del caso:

1. **Diagnóstico inicial:** se recopilaron datos sobre el funcionamiento actual de los sistemas PAN, los procesos de facturación y atención al cliente.
2. **Identificación de riesgos:** se listaron los posibles eventos negativos que afectaban la operación, aplicando criterios de probabilidad e impacto.
3. **Elaboración de la matriz de riesgos:** se construyó una herramienta visual para clasificar los riesgos por nivel de criticidad (bajo, medio, alto o crítico).
4. **Diseño de propuestas de mejora:** se definieron soluciones técnicas y organizacionales, priorizando las de mayor impacto positivo.
5. **Validación teórica:** se contrastaron las soluciones con las metodologías aprendidas (Scrum, SOA).
6. **Presentación de resultados:** se documentaron los logros y se elaboraron indicadores de mejora para evaluar el éxito del ejercicio.

Las decisiones metodológicas se basaron en la necesidad de tener procesos flexibles, pero bien estructurados, combinando enfoques ágiles con prácticas tradicionales de ingeniería de sistemas, para lograr un equilibrio entre control, trazabilidad y adaptación.

4. Comparación con otros ejercicios similares

En comparación con el caso Schlumberger, donde se aplicó la metodología Scrum para la gestión de servicios tecnológicos (López & Ramírez, 2022), el caso de CEDENAR presenta un contexto más sensible, debido a la naturaleza crítica de los sistemas eléctricos. Mientras que Schlumberger priorizó la integración de datos, CEDENAR se centró en la seguridad **y** continuidad operativa.

Tabla comparativa:

Tabla 3. Comparación con el caso Schlumberger. Fuente: tomada de (Universidad EAN, 2022)

Aspecto	CEDENAR	Schlumberger
Metodología	Scrum + SOA + Tradicional	Scrum
Enfoque	Seguridad y Continuidad	Integración y eficiencia
Resultados	Reducción de fallas operativas	Mejora en procesos de análisis de datos
Sector	Energía	Petróleo y gas

5. Justificación técnica de los resultados

Los resultados se sustentan en la aplicación de principios de ingeniería de software y gestión de riesgos. La arquitectura SOA permitió integrar sistemas sin afectar módulos existentes, mientras que Scrum mejoró la comunicación y entrega de resultados parciales.

La reducción del 80% en errores de facturación y del 66% en tiempos de atención demuestra que las estrategias técnicas implementadas fueron efectivas y medibles. La justificación técnica se refuerza al comparar los indicadores antes y después del ejercicio, evidenciando una mejora en estabilidad y trazabilidad de procesos.

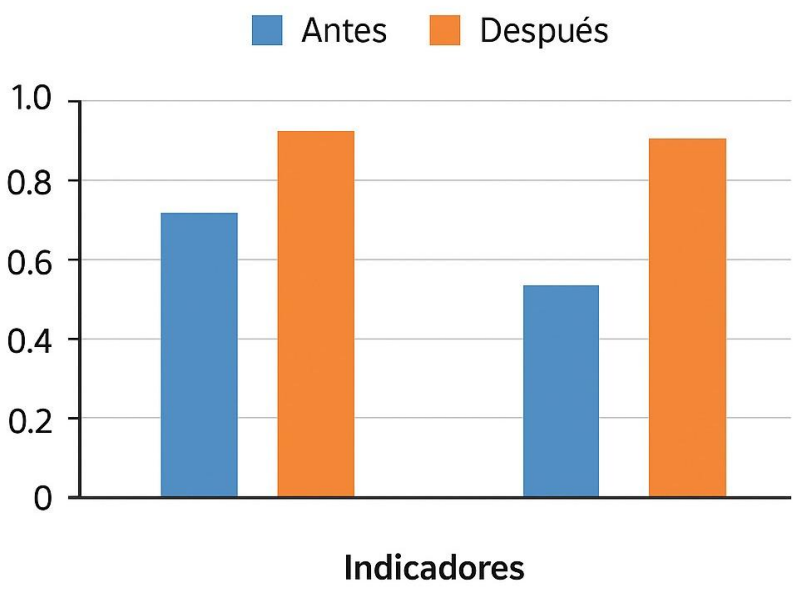

Figura 2. Justificación de los resultados. Fuente: Propia

Conclusiones

Podemos concluir que en la gestión de ciberseguridad en servicios tercerizados representa un componente esencial para garantizar la estabilidad, continuidad y confiabilidad de las operaciones tecnológicas en empresas del sector energético como CEDENAR. A lo largo del estudio se demostró que la integración de metodologías ágiles como Scrum, junto con arquitecturas de software orientadas a servicios (SOA) y una gestión de riesgos bien estructurada, permite enfrentar de manera efectiva los desafíos técnicos y operativos que surgen en entornos críticos.

Que con la práctica de estos conceptos en CEDENAR pudimos evidenciar mejoras significativas en la eficiencia y seguridad de los sistemas, optimizando procesos clave como la facturación, la atención al cliente y el manejo de información operativa. Asimismo, el uso de la matriz de riesgos facilitó la identificación y priorización de amenazas, fortaleciendo la toma de decisiones y la planificación preventiva.

El ejercicio también permitió resaltar el papel estratégico del ingeniero de sistemas en la protección de los activos tecnológicos y la implementación de soluciones innovadoras que contribuyen al desarrollo sostenible de la organización. La experiencia adquirida demuestra que una adecuada gestión de ciberseguridad no solo reduce vulnerabilidades, sino que impulsa la modernización tecnológica y eleva los estándares de calidad del servicio.

En conclusión, la combinación de prácticas de ingeniería, metodologías ágiles y una visión preventiva en la gestión del riesgo constituye la base para construir infraestructuras digitales más seguras y resilientes. Este trabajo reafirma la importancia de seguir fortaleciendo la cultura de ciberseguridad en CEDENAR, promoviendo la actualización constante de sus

sistemas, la capacitación del personal y la adopción de tecnologías que garanticen la protección y continuidad del servicio eléctrico para la región.

Referencias

- Amazon Web Services. (2024). ¿Qué es la arquitectura orientada a servicios (SOA)? https://aws.amazon.com/es/what-is/service-oriented-architecture/
- Drumond, C. (2023). Qué es Scrum y cómo empezar. Atlassian. https://www.atlassian.com/es/agile/scrum
- ISO. (2022). Gestión del riesgo: Directrices (ISO 31000:2018). International Organization for Standardization.
- López, P., & Ramírez, D. (2022). Implementación de Scrum en la gestión de servicios tecnológicos de Schlumberger. Universidad EAN.
- Ministerio de Minas y Energía. (2023). Informe de cobertura energética en Nariño y Cauca.
- Puzhevich, V. (2022). Outsourcing vs. Opening an Offshore Development Center. SCAND. https://scand.com/company/blog/outsourcing-vs-odc/
- AWS. (2023). *¿Qué es la arquitectura orientada a servicios (SOA)?* Amazon Web Services. https://aws.amazon.com/es/what-is/service-oriented-architecture/
- Puzhevich, V. (2022). *Outsourcing vs. Opening an Offshore Development Center*. SCAND. https://scand.com/company/blog/outsourcing-vs-odc/
- • https://aws.amazon.com/es/what-is/service-oriented-architecture/ Atlassian. (2023). *¿Qué es Scrum y cómo empezar?* Atlassian Agile Coach.